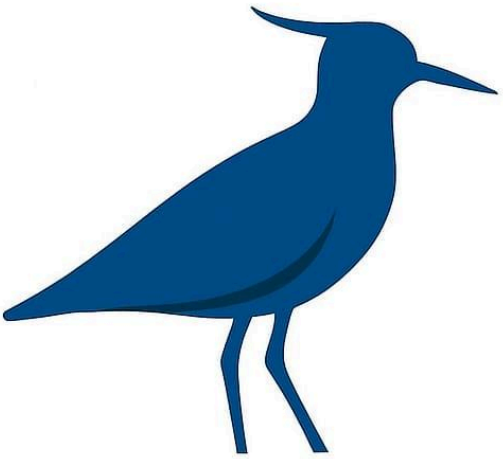

LYNUXBYTE

WEBSITE DEVELOPMENT • URUGUAY

Solicitante: I.T.S - Instituto Tecnológico Superior Arias Balparda.

Nombre Fantasía, de la nueva empresa: Lynux Byte

Grupo: 3°ML

Turno: vespertino

Unidad Curricular: Sistemas Operativos

Nombres de los integrantes del grupo: Nahüm Souza, Leandro Rodriguez, Santiago Fernandez, Yan Boné

Fecha de entrega: 15/09/2025

Instituto Tecnológico Superior Arias Balparda.
Blvr. José Batlle y Ordóñez 3570 esq. Gral. Flores – Montevideo.

Administrador

¿Qué es?

Usuario con privilegios máximos (equivalente a root en Linux), encargado de la instalación, configuración y mantenimiento de todo el sistema.

Responsabilidades y permisos

- **Acciones permitidas**
    - Instalar/eliminar paquetes y servicios.
    - Modificar cualquier fichero del sistema (incluyendo /etc, /usr, /var, /root).
    - Gestionar cuentas de otros usuarios (crear, borrar, cambiar contraseñas).
    - Configurar redes, firewall y acceso remoto.
    - Actualizar el kernel y aplicar parches de seguridad.
- **Acciones denegadas**

- Ninguna a nivel de sistema operativo; sin embargo, puede haber políticas de auditoría o “break-glass” que registren o requieran aprobación previa.

- **Ámbito de operación**

  - Alcance global en servidor y terminales.

  - Acceso habitual vía SSH con clave segura y/o autenticación multifactor.

Modelo de seguridad recomendado

- Uso de sudo en lugar de login directo como root.

- Archivo /etc/sudoers bien definido, limitando comandos críticos.

- Registro de todas las acciones con auditd.

Usuario

¿Qué es?

Cuenta de persona final o servicio genérico con permisos restringidos a su propio entorno.

Responsabilidades y permisos

- **Acciones permitidas**

  - Leer/escribir en su directorio home (/home/usuario).

  - Ejecutar aplicaciones instaladas (navegadores, editores, etc.).

    - Registrar procesos personales y modificar su configuración local (p. ej. ~/.bashrc).

- **Acciones denegadas**

    - Acceder a carpetas de otros usuarios o del sistema (sin elevación).
    - Instalar/eliminar software global.
    - Reiniciar servicios o cambiar configuraciones de red.

- **Ámbito de operación**

    - Limitado a su UID; no puede ver logs de otros usuarios ni ficheros como /etc/shadow.

Notas

- Se añade al grupo primario (usuarios) y a grupos secundarios según necesidades (p. ej. docker, backup).

Grupo

¿Qué es?

Agrupación de cuentas de usuario para facilitar la asignación masiva de permisos.

Responsabilidades y permisos

- **Acciones permitidas**

- Lectura, escritura o ejecución de recursos a los que el grupo tenga permiso Unix (propietario, grupo, otros) o ACL.

- **Acciones denegadas**

  - Lo que no esté explícitamente permitido por los permisos de archivos, directorios o políticas de seguridad.

- **Ámbito de operación**

  - Define derechos de acceso a carpetas compartidas y servicios (p. ej. grupo www-data para el servidor web).

Implementación

- Crear grupos con groupadd.

- Asignar usuarios con usermod -aG nombre_grupo usuario.

- Control fino vía ACL (setfacl/getfacl) si se necesita más granularidad.

“bacap” (usuario de backup)

Nota: asumo que “bacap” es la cuenta encargada de tareas de copia de seguridad.

¿Qué es?

Cuenta de sistema dedicada a ejecutar scripts de copia de seguridad (backups) y restauraciones automatizadas.

Responsabilidades y permisos

- **Acciones permitidas**
    - Leer datos de todos los directorios críticos (/etc, /var/www, /home) para copiar.
    - Montar/desmontar dispositivos de almacenamiento externo (si está en sudoers para ello).
    - Ejecutar herramientas como rsync, tar, borg, restic.
- **Acciones denegadas**
    - Modificar ficheros originales (solo lectura).
    - Cambiar configuraciones del sistema.
- **Ámbito de operación**
    - Puede necesitar permisos de lectura global; se limita su shell con nologin y se ejecutan sus tareas por cron.

Modelo de seguridad

- Incluir en sudoers solo los comandos necesarios (p. ej. /usr/bin/rsync --archive).
- Registrar logs detallados de cada operación de backup.
- Deshabilitar login interactivo (/usr/sbin/nologin).

Rol Docker

¿Qué es?

Grupo o rol que permite a usuarios particulares gestionar contenedores Docker sin ser administradores full (root).

Responsabilidades y permisos

- **Acciones permitidas**
    - Iniciar, detener y eliminar contenedores (docker start|stop|rm).

- Construir imágenes (docker build).
- Etiquetar y subir imágenes a repositorios.
- Ver logs de contenedores.

- **Acciones denegadas**
  - Cambiar configuraciones del demonio Docker (dockerd).
  - Instalar/eliminar el propio paquete Docker.
  - Acceder a ficheros del sistema más allá de los volúmenes mapeados.

- **Ámbito de operación**

Se consigue añadiendo el usuario al grupo docker:

sudo usermod -aG docker nombre_usuario

-
- Tras reiniciar sesión, el usuario puede ejecutar la CLI de Docker sin sudo.

Consideraciones de seguridad

- Elgrupo docker es prácticamente equivalente a root dentro de contenedores:
  - Puede montar directorios arbitrarios desde el host.
  - Conviene limitar su uso a personal de confianza o usar herramientas de orquestación con RBAC (p. ej. Kubernetes).

Tabla comparativa resumida

Rol	UID/GID	Permisos clave	Shell típico	Elevación necesaria
Administrador	UID 0 (root)	Todo el sistema	/bin/bash	No
Usuario	UID ≥ 1000	Solo home y aplicaciones autorizadas	/bin/bash	Sí (sudo limitado)
Grupo	GID ≥ 1000	Depende de permisos de archivos/grupos	N/A	N/A
bacap	UID dedicado	Lectura global, ejecución de scripts backup	/usr/sbin/nologin	Sí (sudo específico)
Docker	GID docker	Gestión completa de contenedores	/bin/bash	No (tras grupo)

12. Hoja testigo:

_____

Firma del Profesor